

## ABSTRACT OF THE DISCLOSURE

## METHOD AND SYSTEM FOR PUBLIC-KEY-BASED

## 5      SECURE AUTHENTICATION TO DISTRIBUTED LEGACY APPLICATIONS

10      A method, a system, an apparatus, and a computer  
program product are presented for an authentication  
process. A host application or system within a  
distributed data processing system supports one or more  
controlled resources, such as a legacy application, that  
requires the receipt of authentication data prior to  
allowing a user to have access to the controlled  
resource. The required authentication data is encrypted  
15      using the public key of the host system, and an attribute  
certificate containing the encrypted authentication data  
is generated by an attribute-certificate-issuing  
authority. When a user of a client application or system  
requires access to the controlled resource, the attribute  
20      certificate is sent to the host, which decrypts the  
authentication data with its private key prior to  
forwarding the authentication data to the controlled  
resource. The controlled resource then authenticates a  
user based on the provided authentication data.

100-620700-1